

AIB: AmRRON Intelligence Brief (white paper) 20 MAR 2024

[supercedes previous white paper dated 07 MAR 2019]

Statement of Purpose: Provide understanding of the AIB as a training tool to provide opportunities for handling real-world intelligence information for network-wide distribution among AmRRON radio operators on a scheduled and consistent basis.

1. The *AmRRON Intelligence Brief (AIB, or 'Intel Brief')* is a weekly (every Monday) distribution of real-world intelligence compiled from reports produced by Forward Observer Early Warning report, Knightsbridge Research, and other trusted sources.
2. The AIB will be initiated by AmRRON National on a weekly basis, as shown in Figure 1, and will be sent as an FLMSG (.k2s) file. It is intended to be received by any available AmRRON operator, and transmitted by NCSs over their regularly-scheduled practice nets over the following week.

MONDAY (weekly)				
FLMSG	@ 2000z	14.110	MFSK-32 (900 on wf)	
FLAMP	@ 2010z	14.110	MFSK-32 (900 on wf)	xmit of .k2s file
FLMSG	@2020z	7.110	MFSK-32 (900 on wf)	
FLAMP	@2030z	7.110	MFSK-32 (900 on wf)	xmit of .k2s file

Figure 1

3. The AIB must be distributed and received over radio or by courier ONLY. Digital modes are strongly recommended, especially those using FEC (Forward Error Correction) modes, such as FLAMP, WINMOR, gARIM, etc. If using Winlink, the message must be sent and received via radio (No TELNET -- this is an honor system).

4. Each weekly AIB will begin as an FLMSG .k2s file and should be between 1.5 and 2k bytes in size.

5. AUTHENTICATION:

5.1 Each AIB .k2s file will be 'hashed' using a CheckSum program. This creates a unique file ID (fingerprint) of the file which allows you to authenticate that the file you've received is not corrupted or altered and is precisely the same file that was transmitted from AmRRON National. The check sum can be compared to the check sum hash posted on the website. Learn how to use check sum utilities at: <https://amrron.com/2019/03/13/white-paper-hashing-files-with-checksum-utilities-tamper-detection/>

5.2 Official AmRRON traffic is also digitally signed using a PGP key, for message traffic received over digital modes with FEC (Forward Error Correction). This allows anyone who has previously downloaded the AmRRON Actual PGP key to authenticate official AmRRON traffic, even if the internet is down. Learn more about PGP signed authentication at: <https://amrron.com/2023/05/21/authenticate-files-using-gpg-gpg-signed-certificates/>

5.3 Additionally, all official AmRRON traffic is accompanied by a separate authentication process shared with Tier 4 and 5 stations, such as most regional HF NCS stations. This allows for authentication among HF NCSs, even if the message traffic was not received over FEC digital modes. For example, message traffic received over plain text, or FLMSG, or voice, can still be checked for authenticity. If not authentic, these stations can alert the network of potential spoofing or erroneous traffic, and prevent the further distribution of questionable traffic, and discredit harmful, misleading, or erroneous traffic presented as official AmRRON traffic.